

PATENTS

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

	Confirmation No:	9526
Applicant:	Eskicioglu, Ahmet Mursit	Atty. Docket: 93418.000034
Application No.:	09/445,133	Examiner: Yogesh Paliwal
Filed:	March 13, 2000	Art Unit: 2135
Title:	GLOBAL CONDITIONAL ACCESS SYSTEM FOR BROADCAST SERVICES	

Mail Stop Appeal Briefs - Patents  
Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450

April 13, 2009 (Monday)

**APPEAL BRIEF**

Appellant hereby appeals to the Board of Patent Appeals and Interferences from the Examiner's final rejection of claims as set forth in the Office Action mailed June 11, 2008.

A timely Notice of Appeal was filed on December 11, 2008, and Appellant hereby petitions under 37 CFR 1.136(a) to extend the due date for filing the Appeal Brief two months, from February 11, 2009, up to and including Monday, April 13, 2009. The requisite fee for the extension of time is being paid concurrently with the filing of this Brief. Nevertheless, the Commissioner is hereby authorized to charge any deficiency, and credit any overpayment, to Deposit Account No. 03-3875.

#### Real Party-in-Interest

UQE, LLC is the real party-in-interest in this proceeding.

#### Related Appeals and Interferences

No appeals or interferences are known which will directly affect or be directly affected by or have bearing on the Board's decision in the pending appeal.

#### Status of the Claims

Claims 1-20 are pending in the application. All of the claims have been finally rejected, and are being appealed herein. Appendix I provides a clean, double-spaced copy of the claims on appeal.

#### Status of Amendments

No amendments were filed in this application subsequent to the final rejection.

#### Summary of Claimed Subject Matter

According to one aspect of the invention, independent claim 1 recites a method for managing access to a scrambled event of a service provider (SP). The method includes receiving in a device (STB 40, 400, 400') an electronic list of events (EPG 58) available from one or more sources (e.g., ISP 56), each event having a digital signature and an encrypted message associated therewith (p. 10, ll. 17-18), receiving in the device, in response to user selection of one of the events from the list of events, the digital signature and the encrypted message associated with the selected event (p. 10, ll. 25-29), the digital signature being encrypted with a first key ( $KCA_{Pri}$ ) and the encrypted message being encrypted with a second key ( $KSC_{Pub}$ ) different from the first key (p. 10, ll. 18-22), the encrypted message comprising a descrambling key ( $KSP_{Event}$ ) and event information including at least one of a channel identity, date and time stamp, event identity and

payment amount corresponding to the selected event (p. 11, ll. 13-15); authenticating in the device a source of the digital signature and the encrypted message associated with the selected event by decrypting the digital signature in response to receiving the digital signature and the encrypted message (p. 10, l. 27 – p. 22, l. 8); decrypting in the device the encrypted message to obtain the descrambling key upon the authenticating (p. 11, ll. 10-15); receiving in the device the selected event from the service provider (p. 11, ll. 21-23), the selected event being scrambled using the descrambling key for preventing unauthorized access to the selected event; and descrambling in the device the selected event using the descrambling key (p. 11, ll. 21-23).

According to another embodiment of the invention, dependent claim 3 recites the method of claim 1 wherein the device comprises a smart card 42 and the steps of decrypting the message, receiving the selected event and descrambling the selected event are performed in the smart card (p. 10-11), and wherein the second key is a first public key associated with the smart card ( $KSC_{Pub}$ ) and the step of decrypting uses a first private key associated with and stored in the smart card ( $KSC_{Pri}$ ), wherein the message further comprises event information, the event information being decrypted using the private key ( $KSC_{Pri}$ ).

In another aspect of the invention, independent claim 15 recites a method for managing access between a device (40, 400, 400') having a smart card (42, 420, 420') coupled thereto and a service provider (SP). The device performs the steps of receiving an electronic program guide (EPG) having a plurality of events from a guide provider, the guide having a message and a digital signature associated with each event in the guide (p. 10, ll. 17-18), the message being encrypted using a public key of the smart card ( $KSC_{Pub}$ ) and the digital signature being created using a private key of the guide provider ( $KCA_{Pri}$ ); selecting an event from the guide (p. 10, ll. 25-27); receiving the encrypted message and the digital signature corresponding to the selected event (p. 10, ll. 27-28); authenticating the guide provider by decrypting the digital signature using a public key of the guide provider ( $KCA_{Pub}$ ), the guide provider public key being stored in the device (p. 10, l. 27 – p. 11, l. 3); passing the message to the smart card (p. 11, ll. 10-11); decrypting, in the smart card, the message using a private key of the smart card to obtain event information and a symmetric key ( $KSC_{Pub}$ ), the smart card private key being stored within the smart card (p. 11, ll. 11-15); storing the event information in the smart card and updating account information based on the event information (p. 11, ll. 15-18); receiving from the service provider the selected event, the selected event being scrambled using the symmetric key; and

descrambling, in the smart card, the selected event using the symmetric key to generate a descrambled event (p. 11, ll. 20-25).

In yet another aspect of the invention, independent claim 18 recites a method for managing access between a device (40, 400, 400') having a smart card (42, 420, 420') coupled thereto and a service provider (SP). The device performs the steps of receiving an electronic program guide having a plurality of events from a guide provider, the guide having a digital certificate and a separate message corresponding to each event in the guide, each of said digital certificates being encrypted using a first private key of the guide, the separate message being encrypted using a public key of the smart card and having an associated digital signature created using a second private key of the guide (p. 12, ll. 4-19); selecting an event from the guide p. 10, ll. 25-27; receiving the digital certificate, the message and the digital signature corresponding to the selected event (p. 12, ll. 4-19); authenticating the guide provider by decrypting the digital certificate using a first public key of the guide to obtain a second public key of the guide, and decrypting the digital signature using the second guide public key, said first guide public key being stored in the device (p. 12, ll. 4-19); passing the message to the smart card (p. 11, ll. 10-11); decrypting, in the smart card, the message using a private key of the smart card to obtain event information and a symmetric key, the smart card private key being stored within the smart card (p. 11, ll. 15-18); storing the event information in the smart card and updating account information based on the event information (p. 11, ll. 15-18); receiving from the service provider the selected event, the selected event being scrambled using the symmetric key; and descrambling, in the smart card, the selected event using the symmetric key to generate a descrambled event (p. 11, ll. 20-25).

#### Grounds of Rejection to be Reviewed on Appeal

1. Whether claim 1 is unpatentable over the combination of the article *IBM Cryptolopes, Super Distribution and Digital Rights Management* (Kaplan) and U.S. Patent No. 6,021,491 (Renaud).
2. Whether claims 2-14 are unpatentable over the combination of *Kaplan, Renaud*, and the article *Cryptology for Digital TV Broadcasting* (Macq).

3. Whether claims 15-17 are unpatentable over the combination of *Kaplan, Renaud,* and *Macq.*

4. Whether claims 18-20 are unpatentable over the combination of *Kaplan, Renaud,* Section 8.3 of the text *Applied Cryptography, Second Edition (Schneier),* and *Macq.*

### Argument

The present invention relates generally to a global conditional access system for broadcast services. More particularly, the invention relates to a system for controlling access to information provided by a service provider to a user.

As described in the Background of the Invention section of the application, content for viewing by a user can come from a number of different service providers. The present invention aims to provide control over content at the device, i.e., at the user-side, to grant and deny access to certain content, and to record uses of the content, when authorization to view is granted.

In one preferred aspect of the present invention, as discussed beginning on page 10 of the application, with reference to Figure 3, a set-top box (STB) 400 is provided that is coupled to a smart card 420. (The invention does not require a smart card 420, as the processing could be done within the STB 400, a digital television, or the like.) The STB 400 receives services from a number of service providers, including, but not limited to, broadcast TV service providers and internet service providers. The STB 400 also is coupled to an electronic event guide (EPG) 580. "EPG 580 may be a separate service provider wherein electronic program guides containing listings of events from a plurality of service providers may be accessed." Page 20, ll. 12-14.

The EPG 580 has a unique digitally signed and encrypted message associated with each event. In a preferred embodiment, the encrypted message includes information corresponding to the selected event and an event key, for decrypting the event chosen from the list. See, p. 10, ll. 17-22.

In operation, a user is presented with a list of the events available for viewing/purchase. Upon selecting one of the events, the digitally signed message is downloaded to the STB 400. The source, i.e., the EPG 580, is authenticated, e.g., by decrypting the digital signature. See, p. 10, l. 27 – p. 11, l. 1.

Having authenticated the EPG, the encrypted message is passed to the smart card 420 for decryption. This decryption obtains the data corresponding to the selected event and the event key. The data is used to update the user account information. The event key is stored in the smart card 420, and is subsequently used to descramble the selected event, when the event is received from the service provider. The descrambled event is thereafter viewed and/or otherwise used by the user. *See*, p. 11, ll. 10-25.

In another embodiment, described on page 12 of the application, the EPG 580' downloads a digital certificate and a digitally signed message to STB 400' when an event is selected. This scenario alleviates the need for a certificate authority to sign every message; it can instead provide a digital certificate for the public key of the service provider. The service provider would then generate digitally signed messages.

As a result of the present invention, the manufacturer of STB is in better control of allowing or denying access to content from various service providers. In this manner, for example, the STB manufacturer is better positioned to share revenues with the service providers.

#### CLAIM 1

Claim 1 stands rejected under 35 U.S.C. § 103, as unpatentable over the combination of *Kaplan* and *Renaud*. Under Section 103, a claimed invention is unpatentable if the differences between it and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the pertinent art.

“[R]ejections on obviousness grounds cannot be sustained by mere conclusory statements; instead, there must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness”, *In re Kahn*, 441 F.3d 977, 988, 78 USPQ2d 1329, (Fed. Cir. 2006). The Examiner has made no showing that claim 1 would have been obvious in view of the combination of *Kaplan* and *Renaud*.

*Kaplan* teaches a cryptographic envelope (cryptolope). As illustrated on page 3, and described on pages 2-4, a cryptolope according to *Kaplan* includes an Abstract, an Encrypted Part (text) with associated Key Record, and Encrypted Part (image) with associated Key Record, Encrypted Fingerprinting and Watermarking Instructions, Terms and Conditions, and

Authenticity (BOM) with Digital Signatures. The Key Records contain document keys for accessing the Encrypted Parts, and the document keys are encrypted using a master key.

When a user desires to view the Encrypted Parts (text and/or images) contained in the cryptolope, he initiates a transaction with, for example, a website. The process of purchasing is described on page 7 of *Kaplan*, and includes creating a buy request cryptolope containing a Bill of Materials, Terms and Conditions for getting the information, and the key records, as well as user credentials. The buy request cryptolope is then sent to a clearing center that verifies the transaction, and thereafter decrypts the key files and re-encrypts the document keys under the public key of a module of the user. These encrypted document keys are then sent back to the user, where they are decrypted and used for accessing the encrypted information.

*Kaplan* does not teach or suggest many features of independent claim 1. For instance, nowhere does *Kaplan* teach or suggest at least receiving in a device a digital signature and encrypted message associated with an event in response to a selection of the event from a list of events, the encrypted message including a descrambling key and event information including at least one of a channel identity, date and time stamp, event identity and payment amount corresponding to the selected event.

As best understood, the Examiner has taken the position, on pages 2, 3, 5, and 6 of the Final Office Action that the claimed encrypted message is taught by one or more of the Encrypted Part (text), the Encrypted Part (image), the Key Records, and the Encrypted fingerprinting and watermarking instructions. Appellant disagrees.

The claimed "encrypted message" cannot be taught by or obvious from either of the Encrypted Parts, because there is no teaching in *Kaplan* that the Encrypted Part includes a descrambling key and event information. Claim 1 recites that the encrypted message comprises a descrambling key and event information. In *Kaplan*, the Encrypted Parts are the digital works purchased using the cryptolope system; they would not include a descrambling key and event information. Thus, the claimed encrypted message is not taught by the Encrypted Parts of the cryptolopes.

The claimed encrypted message also is not taught by the Key Records. While the Key Records of *Kaplan's* system do include keys used to descramble content, i.e., to descramble the

Encrypted Parts, the Key Records do not include event information. Claim 1 recites that the “encrypted message compris[es] a descrambling key and event information....”

The claimed encrypted message also is not taught by the Encrypted Fingerprinting and Watermarking Instructions. As described in *Kaplan* at page 5, the Encrypted Fingerprinting and Watermarking Instructions are included as a “‘post-processing’ algorithm which is applied to the protected content of the cryptolope as it is decrypted and before it is presented to the user.” The algorithm creates “a unique, customized version of the cryptolope’s protected content for each user that ‘buys’ (or licenses the right to use the contents of) the cryptolope.” The Encrypted Fingerprinting and Watermarking Instructions are provided so that content purchased by a user is traceable to that user. The Instructions do not include a descrambling key or event information, as featured in claim 1.

Thus, none of the Encrypted Parts, the Key Records and the Fingerprinting and Watermarking Instructions is understood to include event information. Accordingly, none contains both a descrambling key and event information.

With regard to the event information of claim 1, the Examiner has taken the position, on page 6 of the last Office Action, that the Terms and Conditions and the Encrypted Fingerprinting and Watermarking Instructions teach this feature.

The Terms and Conditions of *Kaplan* are specified by the publisher of the cryptolope and govern access of potential users to the encrypted, protected content of the cryptolope. These Terms and Conditions could be used to limit access, to charge a rate for access, or to control redistribution, for example. Even if the Terms and Conditions and the claimed event information contain similar information, however, the Terms and Conditions are not contained in an encrypted message, as featured in independent claim 1. In fact, *Kaplan* teaches that the “T&Cs should usually be presented in ‘human readable’ form to the user.” There is no suggestion anywhere in *Kaplan* that the T&Cs should be encrypted, or included in an encrypted message. Moreover, the Examiner has made no showing as to why this would have been obvious.

*Kaplan* also fails to teach that the encrypted message is encrypted using a second key different from a first key (which encrypts the digital signature). The Examiner has taken the position that page 3, lines 14-15 of *Kaplan* teach this features. This portion recites “[e]ach document key is encrypted under a master key. The resulted encrypted document keys are stored



in key records within the cryptolope.” However, all that this portion of *Kaplan* teaches is that document keys are encrypted. It does nothing to teach using a second key to encrypt an encrypted message comprising a descrambling key and event information.

The Examiner seems to be picking and choosing portions of *Kaplan* and attempting to arbitrarily assign them to features of independent claim 1, with mere conclusory statements of obviousness. However, and as just demonstrated, the rejection still fails to teach or render obvious at least the encrypted message of claim 1, and no showing has been made as to why this feature would have been obvious.

*Renaud* does nothing to remedy the deficiencies of *Kaplan*. *Renaud* relates to digital signatures for data streams and data archives. While *Renaud* may teach user-verification of a signature, it does not teach or suggest at least the encrypted message of claim 1 or that the encrypted message is encrypted using a second key different from a first key.

For the foregoing reasons, Appellant submits that the combination of *Kaplan* and *Renaud* fails to teach or suggest features of independent claim 1. Claim 1 is allowable.

#### CLAIMS 2 and 4-14

Claims 2 and 4-14 depend from claim 1 and are submitted to be allowable because of this dependency, and for reciting other patentable features of Appellant’s invention.

#### CLAIM 3

Claim 3 recites all features of claims 1 and 2, and further that the event information contained in the message is decrypted using the private key (of the smart card). Nowhere is this feature taught or suggested by the combination of *Kaplan*, *Renaud*, and *Macq*.

*Kaplan* is cited for teaching “the message further comprises event information, the event information being decrypted using the private key (Page 3).” However, *Kaplan* does not teach on page 3 encrypting event information. The Examiner has previously taken the position that the event information is taught by the Terms and Conditions of *Kaplan*, but *Kaplan* does not teach encrypting the Terms and Conditions with a private key. *Kaplan* does not teach encrypting

the Terms and Conditions at all. To the contrary, *Kaplan* notes that the Terms and Conditions should be in a “human readable” format, presumably so the purchaser of the cryptolope knows the terms and conditions prior to purchase.

*Renaud* and *Macq* also do not teach decrypting event information, as recited in dependent claim 3. Accordingly, claim 3 is believed to be patentable.

### CLAIM 15

Claim 15 stands rejected under 35 USC Section 103 as unpatentable over the combination of *Kaplan*, *Renaud*, and *Macq*. Appellant disagrees.

Claim 15 recites a method for managing access between a device having a smart card coupled thereto and a service provider. Among other features, claim 15 recites receiving an electronic program guide from a guide provider, the guide having a message and a digital signature associated with each event in the guide, the message being encrypted using a public key of the smart card; and decrypting, in the smart card, the message using a private key of the smart card to obtain event information and a symmetric key, the symmetric key being used to descramble the selected event. Many of the features of claim 15 are not taught or rendered obvious by the asserted combination.

Specifically, the Examiner has acknowledged, at page 14 of the last Office Action, that “*Kaplan* does not disclose ... decrypting, in the smart card, the message using a private key of the smart card to obtain event information and a symmetric key....” On page 15 of the Office Action, the Examiner alleges that a portion of *Macq* teaches “decrypting, in the smart card, the message using a private key being stored within the smart card.” Even assuming that the Examiner’s characterization of *Macq* is correct in this regard, the Examiner has made no showing that the message is decrypted “to obtain event information and a symmetric key,” as recited in claim 15.

On page 4 of the last Office Action, in response to previously-filed arguments, the Examiner stated that “both the key record and encrypted fingerprinting and watermarking instructions are decrypted and decryption of key record does reveal the symmetric key ... which is used to descramble a scrambled event.” Even if decrypting the Key Records of *Kaplan* does

reveal a symmetric key, it does not “obtain event information and a symmetric key,” as recited in claim 15. There also is no teaching that the Encrypted Fingerprinting and Watermarking Instructions are decrypted to obtain event information and a symmetric key. The Examiner also has made no showing as to why this would be obvious from the cited references.

For the foregoing reasons, Appellant submits that claim 15 is patentable over the asserted combination of *Kaplan*, *Renaud*, and *Macq*.

#### CLAIMS 16 and 17

Claims 16 and 17 depend from claim 15 and are submitted to be allowable because of this dependency, and for reciting other patentable features of Appellant’s invention.

#### CLAIM 18

Claim 18 stands rejected under 35 USC Section 103 as unpatentable over the combination of *Kaplan*, *Renaud*, *Schneier* and *Macq*. Appellant disagrees.

Claim 18 recites a method for managing access between a device having a smart card coupled thereto and a service provider. Among other features, claim 18 recites receiving an electronic program guide from a guide provider, the guide having a digital certificate and a separate message corresponding to each event in the guide, the separate message being encrypted using a public key of the smart card and having an associated digital signature created using a second private key of the guide; and decrypting, in the smart card, the message using a private key of the smart card to obtain event information and a symmetric key, the symmetric key being used to descramble the selected event. Many of the features of claim 18 are not taught or rendered obvious by the asserted combination.

Specifically, the Examiner has acknowledged, at page 18 of the last Office Action, that “*Kaplan* does not disclose ... decrypting, in the smart card, the message using a private key of the smart card to obtain event information and a symmetric key....” On page 19 of the Office Action, the Examiner alleges that a portion of *Macq* teaches “decrypting, in the smart card, the message using a private key being stored within the smart card.” Even assuming that the Examiner’s characterization of *Macq* is correct in this regard, the Examiner has made no

showing that the message is decrypted “to obtain event information and a symmetric key,” as recited in claim 18.

On page 4 of the last Office Action, in response to previously-filed arguments, the Examiner stated that “both the key record and encrypted fingerprinting and watermarking instructions are decrypted and decryption of key record does reveal the symmetric key ... which is used to descramble a scrambled event.” Even if decrypting the Key Records of *Kaplan* does reveal a symmetric key, it does not “obtain event information and a symmetric key,” as recited in claim 18. There also is no teaching that the Encrypted Fingerprinting and Watermarking Instructions are decrypted to obtain event information and a symmetric key. The Examiner also has made no showing as to why this would be obvious from the cited references.

The cited art also does not teach or suggest that each event has associated with it a digital certificate encrypted using a first private key of the guide and a separate message, having a digital signature created using a second private key of the guide. As best understood, *Kaplan* teaches attaching a digital signature to a Bill of Materials, not to a message that is subsequently decrypted to obtain event information and a symmetric key.

For the foregoing reasons, Appellant submits that claim 18 is patentable over the asserted combination of *Kaplan*, *Renaud*, *Schneier*, and *Macq*.

#### CLAIMS 19 and 20

Claims 19 and 20 depend from claim 18 and are submitted to be allowable because of this dependency, and for reciting other patentable features of Appellant’s invention.

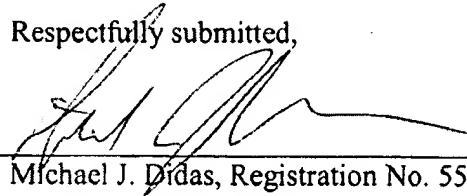
#### Summary

The cited art, whether taken alone or in proper combination, fails to teach all of the limitations of Appellant’s claims.

Conclusion

For the foregoing reasons, Appellant respectfully requests that the Board of Patent Appeals and Interferences reverse the rejection by the Examiner and mandate allowance of the claims.

Respectfully submitted,



---

Michael J. Didas, Registration No. 55,112

Customer Number 23387

HARTER SECREST & EMERY LLP

1600 Bausch & Lomb Place

Rochester, New York 14604

Telephone: 585-232-6500

Fax: 585-232-2152

## APPENDIX I – CLAIMS ON APPEAL

1. (Previously Presented) A method for managing access to a scrambled event of a service provider, said method comprising:

receiving in a device an electronic list of events available from one or more sources, each event having a digital signature and an encrypted message associated therewith;

receiving in the device, in response to user selection of one of the events from the list of events, the digital signature and the encrypted message associated with the selected event, the digital signature being encrypted with a first key and the encrypted message being encrypted with a second key different from the first key, the encrypted message comprising a descrambling key and event information including at least one of a channel identity, date and time stamp, event identity and payment amount corresponding to the selected event;

authenticating in the device a source of the digital signature and the encrypted message associated with the selected event by decrypting the digital signature in response to receiving the digital signature and the encrypted message;

decrypting in the device the encrypted message to obtain the descrambling key upon the authenticating;

receiving in the device the selected event from the service provider, the selected event being scrambled using the descrambling key for preventing unauthorized access to the selected event; and

descrambling in the device the selected event using the descrambling key.

2. (Previously Presented) The method of Claim 1 wherein the device comprises a smart card and the steps of decrypting the message, receiving the selected event, and descrambling the selected event are performed in the smart card, and

wherein the second key is a first public key associated with the smart card and the step of decrypting uses a first private key associated with and stored in the smart card.

3. (Previously Presented) The method of Claim 2 wherein the message further comprises event information, the event information being decrypted using the private key.

4. (Previously Presented) The method of Claim 3 further comprising the step of storing the event information, wherein the step of storing the event information is performed in the smart card.

5. (Previously Presented) The method of Claim 4 wherein the smart card has a card body having a plurality of terminals arranged on a surface of the card body in accordance with one of ISO 7816 and PCMCIA card standards.

6. (Previously Presented) The method of Claim 5 further comprising authenticating the list of events to verify the origin of the message.

7. (Previously Presented) The method of Claim 6 wherein the first key is a second private key and the step of authenticating comprises decrypting the digital signature using a second public key that is stored in the device.

8. (Previously Presented) The method of Claim 4 wherein the event information comprises channel identification data, event identity data, date and time stamp data, and billing data.

9. (Previously Presented) The method of Claim 3 further comprising the step of storing the event information, wherein the step of storing the event information is performed in the device.

10. (Previously Presented) The method of Claim 7 wherein the digital signature, the second public key and the second private key are issued by an independent certificate authority and are associated with the list provider.

11. (Previously Presented) The method of Claim 10 wherein the device is a digital television.

12. (Previously Presented) The method of Claim 10 wherein the device is a set-top box.

13. (Previously Presented) The method of Claim 4 wherein the event information is used within the device to update a user's account information.

14. (Previously Presented) The method of Claim 13 wherein the event information is downloaded to an independent billing center to update the user's account information.

15. (Previously Presented) A method for managing access between a device having a smart card coupled thereto and a service provider, the device performing the steps of:

receiving an electronic program guide having a plurality of events from a guide provider, the guide having a message and a digital signature associated with each event in the guide, the message being encrypted using a public key of the smart card and the digital signature being created using a private key of the guide provider;

selecting an event from the guide;

receiving the encrypted message and the digital signature corresponding to the selected event;

authenticating the guide provider by decrypting the digital signature using a public key of the guide provider, the guide provider public key being stored in the device;

passing the message to the smart card;

decrypting, in the smart card, the message using a private key of the smart card to obtain event information and a symmetric key, the smart card private key being stored within the smart card;

storing the event information in the smart card and updating account information based on the event information;

receiving from the service provider the selected event, the selected event being scrambled using the symmetric key; and

descrambling, in the smart card, the selected event using the symmetric key to generate a descrambled event.

16. (Original) The method of Claim 15 wherein the device is a set-top box.

17. (Original) The method of Claim 15 wherein the device is a digital television.



18. (Previously Presented) A method for managing access between a device having a smart card coupled thereto and a service provider, the device performing the steps of:

receiving an electronic program guide having a plurality of events from a guide provider, the guide having a digital certificate and a separate message corresponding to each event in the guide, each of said digital certificates being encrypted using a first private key of the guide, the separate message being encrypted using a public key of the smart card and having an associated digital signature created using a second private key of the guide;

selecting an event from the guide;

receiving the digital certificate, the message and the digital signature corresponding to the selected event;

authenticating the guide provider by decrypting the digital certificate using a first public key of the guide to obtain a second public key of the guide, and decrypting the digital signature using the second guide public key, said first guide public key being stored in the device;

passing the message to the smart card;

decrypting, in the smart card, the message using a private key of the smart card to obtain event information and a symmetric key, the smart card private key being stored within the smart card;

storing the event information in the smart card and updating account information based on the event information;

receiving from the service provider the selected event, the selected event being scrambled using the symmetric key; and

descrambling, in the smart card, the selected event using the symmetric key to generate a descrambled event.

19. (Original) The method of Claim 18 wherein the device is a set-top box.

20. (Original) The method of Claim 18 wherein the device is a digital television.

## APPENDIX II – EVIDENCE

None.

### APPENDIX III – RELATED PROCEEDINGS

None.